Issue 3 - July 2013

The blackfoot Quarterly

ADVISE >

ASSESS >

ASSURE >

Welcome

Hello and welcome to the Summer 2013 Blackfoot newsletter. Time is flying by and this is now our third newsletter sharing some topical updates as well as the opinions of Blackfoot. Hopefully you are finding these both enjoyable and thought provoking. If you have any feedback or thoughts about topics you would like to hear about please do not hesitate to tell us what is on your mind.

We have a bumper issue for you this time and we bring you the quarterly updates and articles. We are focusing on an issue with a desktop BIOS extension, discussing Secure Software Development and the latest release of the OWASP Top 10.

So let's delve straight in with thoughts from our CEO Matthew Tyler.

I recently conducted an education seminar, which was a left of field look at PCI compliance and UK retail. It was a lighthearted talk and very well received. So I thought I would share some of the points where people have requested more information.

Should the PCI standard apply in the UK ? Face to face card fraud around the world is increasing year on year. It was up 2.3% in the US, 23% in Russia and 36% in China. The US now accounts for 25% of transactions and 60% of fraud. However in the UK since its peak in 2004 it has fallen by over 80%, due to the implementation of Chip and Pin. Total face to face fraud in the UK was down to £43M in the UK. This roughly equates to around £4.30 per end point, or around 0.038% of transaction value. Why would you spend any more than that to protect it?

Overall UK Fraud figures stand at around £73B and of that card fraud is only £280M.
Fraud in UK retail consists of £2.6B customer theft, £1.7B staff theft, £190M in supplier fraud and only £120M in card fraud. So do not tell your boards that this is a massive issue.

There are vested interests everywhere and we are told about new threats daily. In the UK we are spending over £3B per annum on IT security rising at 10% per year, however according to the ICO we have had a tenfold increase in the amount of data breaches.
This leads to the conclusion that IT security spend is in the wrong place.

We are now putting everything on a web application, but still most breaches occur as a result of the OWASP top 10 NOT being in place. These vulnerabilities are unchanged in 10 years. How can this be right?

My slides are now available to download on our website or if you would like us to personally present this then please give me a call.

Matthew Tyler
Blackfoot CEO

Quarterly Review

The PCI Security Standards Council has been quiet recently as the new version of the standard is released in October. However the first PCI P2PE applications have been certified in the UK. Listings of all validated applications will be on the PCI Security Standards Council website, www.pcisecuritystandards.org. There are still no solutions accredited so those of you expecting to take the plunge this year may be disappointed.

For those with an interest in card fraud the UK Cards Association have now released the 2012 figures. Whilst there has been a 14% rise in fraud it still only accounts for 7p in every £100 spent on cards. Low tech crime is on the increase so watch out for cold calls and be vigilante when using ATMs. The full report can be found at http://www.theukcardsassociation.org.uk/news/FYFF2012.asp

Blackfoot is starting see an increase in web hosts and infrastructure providers being more stringent when clients have penetration testing work conducted. More notice period, details of the testers, testing window information, testing contracts and more. So if you are thinking about having any penetration testing conducted you need to ensure you know what your third party requirements are. Work with both your provider and tester to ensure that it runs smoothly. Should you have any questions please contact us.

Articles

BIOS Extension

Last year we, and others found a security concern on desktop PC's. As nothing much has been heard since we have decided to raise it up again via the newsletter.

Our client had bought branded desktop PC's in batches from the manufacturer to a standard specification, but this had been interpreted by the manufacturer as a "baseline" specification and many systems had been delivered to a specification exceeding the baseline with, for example, better graphics cards and better CPU's.

Specific to this vulnerability, however, some systems were delivered with the a centralised management tool "Intel Management Engine BIOS Extension (MEBx)" installed and active with a default password (which is easily guessed and freely available on the Internet). This is normally a built-to-order additional option and is typically a chargeable extra. The customer had no knowledge of the presence of this unwanted extra on their machines. MEBx is part of Intel Active Management Technology (http://en.wikipedia.org/wiki/Intel_Active_Management_Technology).

The MEBx is a powerful tool for centrally managing large numbers of systems and allows "out of band" (i.e. without operating system knowledge or control) access to many aspects of the system including remotely:

- Read and change the BIOS settings
- Boot the system from an alternative image to the normal startup
- Access the system console allowing software upgrades and changes
- Remote KVM (Keyboard, Video and Mouse) access
- Access network traffic transmitted and received by the system
- Create hardware and software inventories of the system

Effectively, the unknown presence of MEBx created a "backdoor" to many desktops and resulted in a significant security vulnerability. Most manufacturers have implemented MEBx or variants to support centralised management platforms such as Intel Active Management Technology.

Pressing <Ctrl><p> at boot time appears to be only way to know whether MEBx is installed or not.
If you do not use this tool you may not know it is installed so please check your estate.

Application Security

In the previous newsletters we have banging the drum on secure software development and application security. You will be pleased to hear that we are carrying on in this edition too.

The cost of network security is increasing; the attackers are becoming more persistent and better equipped; so you need improved defences to reduce the risk of successful attacks.

It is highly likely you are getting daily phone calls from people trying to sell you the latest silver bullet for compliance or security, and whilst some are better than others nothing will cure all of your ills.

According to the latest Verizon Data Breach Report 69% of hacking attacks in EMEA were involving SQL injection. The SpiderLabs 2013 Global Security Report puts SQL injection involved in 73% of breaches. This attack is 10 years old so why is this still so common? It is because applications are being poorly developed and not following OWASP or SANS best practice. Functionality, usability and cost remain the leading thoughts in the mind rather than security.

If you outsource your application development ensure that your contract covers secure coding requirements and reference best practice. Likewise, if you develop your own applications make sure your teams are following best practice too. You should follow up that work with an independent code review.

If you are looking to move your business into the cloud, then having securely coded applications with a Secure Software Development Lifecycle supporting them will enable you to make this switch with confidence. There are clear benefits for moving to the cloud but security remains a concern. If you have made the move already what does your contract say about the responsibility of security? Many will say they are not providing the security or if they provide some they are not liable for any costs if something goes wrong. At best you may have some discount if applications are not available. However does this really cover the cost of a website that is unavailable to your customers? Does it even cover the liability of breach penalties? The answer to both is likely to be negative. Before moving to the cloud consider how your applications are today, and if you do not have a secure software development lifecycle now is the time to start thinking about it.

OWASP Top 10

Many of you will have heard of the OWASP Top 10, and we are fortunate enough to have Colin Watson as one of our Senior Consultants who can explain a bit more about it. After all who better to talk about the top 10 than somebody who received an outstanding achievement award from OWASP in 2011?

The Open Web Application Security Project (OWASP) has released the 2013 edition of its well-known top ten list of risks to web applications. This documents attempts to identify an overall summary of the most serious risks across all sectors and types of web application. In this regard it is more of an awareness document, and is very much targeted at those involved with software development.

Due to the general nature of the risks, each item in the OWASP Top Ten is actually quite a large bucket of problems, and it is important for organisations to not only to think about these ten, but to actually determine the actual risks to their own applications. The 2013 OWASP

Top Ten is:

A1 Injection
A2 Broken Authentication and Session Management
A3 Cross-Site Scripting (XSS)
A4 Insecure Direct Object References
A5 Security Misconfiguration
A6 Sensitive Data Exposure
A7 Missing Function Level Access Control
A8 Cross-Site Request Forgery (CSRF)
A9 Using Known Vulnerable Components
A10 Unvalidated Redirects and Forwards

The overall list is not dissimilar to previous versions (2004, 2007 and 2010), and there has been some merging of risks, and splitting out individual items to highlight them. For example, "Insecure Cryptographic Storage" and "Insufficient Transport Layer Protection" from 2010 have been merged into the new A6 "Sensitive Data Exposure".

The OWASP Top Ten is well-known to ecommerce merchants since a previous version became enumerated in PCI DSS Requirement 6.5 "Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes.". Bear in mind that ten issues are not sufficient alone to meet PCI DSS compliance for this requirement, nor of course for more general security assurance. The OWASP Top Ten provides "what next" recommendations for developers and verifiers, and how organisations should go about building application security into their software development processes.